



## **White Paper**

# **Dartmouth College: Realizing a Campus-wide Video and Voice Network**

Brad Noblet  
CIO, Dartmouth College

---

## Introduction

Over the past five years at Dartmouth College, Brad Noblet, CIO of Dartmouth College developed the industry's first totally converged wireless IP network. This paper is intended to provide some insight into the vision behind its deployment and to provide a collection of "best practices" learned from that experience

## Vision

Nothing in life happens without purpose, a guiding beacon that drives innovation. For Dartmouth, it was the necessity to upgrade our tired, creaking information and communications infrastructure. In higher education, information technology (particularly network access) drives how we live, work and play. It's hard to imagine college life without a connection to the Internet. Those who are around a college for any length of time quickly realize that higher education *is* the quintessential example of a mobile society. Due to real estate constraints, space is always at a premium; thus folks are always shifting to find the right space (or even any space) to occupy, if only for a brief moment.

As we began to look at upgrading our network, we traveled two roads. The first was to look beyond the horizon to sneak a glimpse at what would drive next-generation network architecture. Within moments we began to see the world converging.

Since the dawn of Mosaic (and the World Wide Web), more and more applications are integrating or "converging" different forms of communications. The goal is to be more impactful, to make sure messages are getting across for all to understand. Audio, video, graphics, animation, and 3D all play a part in the delivery. On the horizon, we saw the convergence of devices; cell phones and PDAs were beginning to integrate audio, video, email, Personal Information Manager and location awareness all in one package.

Secondly, as we looked at traditional infrastructure that would feed these next-generation applications and devices, we quickly realized that the infrastructure wasn't converged at all. Voice (audio), video, data (graphics), security, and environmental (HVAC) applications were all disparate--all islands unto themselves. Yet, these separate islands would ultimately be called upon to feed these newly converged devices and applications. How would that be possible?

---

More forbidding than the technology challenges were the economic considerations. As we began to look at the cost of re-architecting (and thus re-capitalizing) each of our major networks, the economics looked daunting; \$3 million to upgrade the data (IP) network, \$4 million to upgrade the voice PBX and \$1.5 million to upgrade the CATV (video) network. Then after spending \$8.5 million, the resulting infrastructure would still remain disparate, unable to feed those hungry, converged applications and devices. On top of that, each infrastructure could not provide ubiquitous mobility, even within its own domain. There had to be a better way.

After much research and experimentation, our “vision” was beginning to clear. Applications and operating systems were developing core technologies and APIs that were enabling services that once ran on disparate infrastructure to become mere applications on an IP network. Many of these are familiar to computer-literate users of communication and information technology: MP3, MPEG2, and next-generation MPEG4 applications. Network protocols were evolving as well, with the goal of delivering a “quality of service” commensurate with what was previously provided by the non-converged infrastructure.

Convergence in communications was becoming possible. It would allow us to build and operate one infrastructure in the future. It would enable us to feed from one source all the information demanded by next-generation converged applications and devices.

The Vision was now clear. Build a converged network that matches the needs of next-generation applications and devices and meets the connectivity demands of our mobile society.

When re-architecting a communications and information network, creating a vision from the start is essential. It forces you to look beyond today into the future. It makes you think about what you’re trying to accomplish. It will allow you to communicate and justify your intentions more clearly. The end result is that the wireless infrastructure you craft will be viable for years to come.

---

## Planning

With a vision clearly in mind, it's time to start planning your wireless services. Unfortunately there are no shortcuts. Every situation is different. Service offerings, coverage areas, geography, bandwidth consumption and other factors may vary dramatically from site to site. That's why it's important to have a good understanding of the following:

Who and where is the potential wireless population to be served?

What is their size and demographics (as related to IT)? Where are they located? How are they likely to use wireless? Will you serve outdoor spaces as well as indoor and what is their proximity to the wired network?

The answers to these questions will help you plan the performance and scale of your network. Knowing as much as possible about your wireless users will help you determine how they will use wireless now and in the future. This will help you synthesize design requirements for access, performance and scale of your wireless infrastructure.

Will you serve outdoor spaces as well as indoor?

Deploying wireless outdoors may require additional considerations--a key being the proximity to the wired network backbone. Experience has shown that many buildings enclose or adjoin outdoor areas of interest, making it possible to serve an outdoor space from an indoor window. Understanding the topography and potential AP locations/mounting options may also dramatically affect your outdoor coverage. Be sure to make outdoor coverage part of your plan even if you don't intend on deploying coverage Day One.

What services will you offer?

Will wireless be an overlay service offered as a convenience to supplement existing wired service or will it achieve parity with your wired access? Will your wireless deployment be ubiquitous or regionalized?

Considering the performance of today's wireless infrastructure, that infrastructure may be capable of achieving parity with your wired network access. As such you may find that your population rapidly adopts wireless as its primary service delivery vehicle. Will your network be ready?

---

Considerations such as these demonstrate why it's important to take some time to determine the various applications and services that may be used wirelessly. Knowing this information with as much granularity as possible will allow you to design a well performing and scaleable wireless infrastructure.

Will you support service types that include real-time, latency-sensitive traffic such as video and voice (audio) in addition to email, web surfing, client/server applications and others? Real-time services demand guaranteed delivery times, and services such as video can demand a great deal of wireless bandwidth. Understanding how these services will be used can help your design. For example, the choice between broadcast video and video-on-demand will have a dramatic impact on bandwidth consumption. You must determine the extent to which your population will use these services, during what times and in what geographic locations.

What are your security views or policy?

Security can be a mixed bag. On one hand, everyone wants to be secure. On the other hand, many are not willing to tolerate the overhead that security can place on access or communications. You must determine where you are on this curve. You must also assess your current security infrastructure, particularly access control, and determine its compatibility with wireless mechanisms such as 802.1x.

Will you offer converged services?

One major advantage of an IP network is its ability to converge services into one communications utility. Disparate voice, video and data networks may now be converged into one IP communications utility, saving a great deal of capital and operating expense as well as personnel. Once converged on IP, deploying these services wirelessly is extremely practical thanks to the magic of wireless switching. Wireless convergence offers several advantages including rapid service deployment for new construction or to serve areas where wired service is not feasible or economically viable.

Is presence in you future?

When we communicate electronically, very little is known about the context in which that communication takes place. If we could add information about our location (from which we may infer what we're doing as well), our communications could be enhanced. For example, if we knew a wireless web user to be in a particular location at a particular time, we might deliver to them a targeted piece of information unique to that location and time of day. As location, time or both change, the context would change and the information delivered would change to match the context. Location awareness is now available

---

ubiquitously and cost effectively within your wireless infrastructure. However, you must plan in advance for the inclusion of location services as those plans can affect AP placement and density. You must determine where these services are to be delivered and how granular they need to be.

Based on these parameters, the goal is to develop a geographical map that includes population density and bandwidth consumption derived from service types to help synthesize AP population, density and placement.

Have you really looked into the future?

We are a mobile society and as a result, wireless technology has seen rapid adoption rates. Don't underestimate your population's appetite for wireless. If your coverage is not ubiquitous Day One, at least spend time up front to plan as though it will grow to become ubiquitous. Applications are converging, concurrently consuming video, audio, graphics, interactivity, etc. Devices are converging too. At some point you may be forced to deliver converged services wirelessly as your population migrates to these converged wireless devices and applications. You should spend some time considering the affects of convergence on your wireless design. Its economic impact is much less than you might think and you may find building such an infrastructure Day One to be to your advantage.

Personnel considerations

With every new technology comes the requirement for skilled resources to plan, design, install and maintain that technology. Wireless is no different in that regard. However, the technology does offer some advantages that can simplify the learning process. Because it is based on IP and related standards, your existing IP networking staff can easily learn the specifics pertinent to a wireless network. In addition, their existing skills should be augmented with some radio frequency (RF) training so that they understand the fundamentals of radio wave propagation. Today's planning tools contain much of the RF knowledge required to design a network, but a fundamental understanding of RF technology can assist greatly in deploying and troubleshooting your wireless infrastructure.

## Funding Justification and Acquisition

Experience has shown that it is fairly straightforward to justify a wired infrastructure investment, including the expense of converging voice and video onto that infrastructure. Wires have been the "accepted" practice for interconnecting IT resources-- and major savings can be achieved by collapsing disparate voice and video networks into one converged communications

---

utility. However, wireless has been and often still is viewed as a luxury. Its use is based mainly on productivity and convenience gains, which can be subjective and difficult to quantify. As such, the return on investment (ROI) for wireless is often ill defined. This makes justifying wireless more of a challenge but certainly not an impossibility.

The good news is that more people are experiencing a positive experience with wireless at home. When returning to work, they become distressed that wireless is not ubiquitous (or, in some cases, even available) in the workplace. This pressure can be used to your advantage when seeking funding support for wireless. When seeking support for wireless, consider the following justifications as they relate to your environment:

#### Moves, adds and changes

In an enterprise or campus, moves, adds and changes tend to dominate much of daily operational activities. Given its inherent mobility, wireless can mitigate that. Service need not be repeatedly terminated, then restored. This can have a positive impact on IT staffing requirements

#### Smart Media Venue/Smart Classroom

There is much expense involved in building a smart, rich media facility for the enterprise or campus. These facilities typically command upwards of \$100,000 in equipment alone plus the cost of the venue itself which could be \$500,000 to \$1 million. Once built, these expensive venues become a congested resource, which can be difficult to schedule and manage.

In contrast, consider the power of a laptop coupled wirelessly to a server. This combination creates a ubiquitous "smart classroom" without the expense and limited availability of a dedicated space. Now virtualized, the Smart Media Venue is available anywhere the wireless network may reach.

#### The cost of wiring a building

The cost of re-wiring a three- to four-story office building with Category 5 wire can be as much as \$100,000. Deploying a wireless infrastructure to serve the same location could be done for as little as \$20,000.

#### Providing early or temporary service

---

Many times, buildings become occupied before communications services are completed. Deploying wireless in or near the building of interest can provide access to communications immediately. If communications is fully converged over wireless then users have access to telephone (voice), video and data (Internet, email) services Day One.

## Wireless Network Design

Today's generation of planning tools takes most of the guess work out of wireless network design. AP density and placement are determined automatically based on information gathered in the planning stage. The more detailed and granular the information, the more accurate your design will be.

For the scale of an enterprise or campus, a wireless switching architecture is the only viable option today. It contains the intelligence to help deploy the massive number of APs you will need to serve an enterprise/campus. Plus it's the only effective way to manage deployed bandwidth and to converge services over wireless. Based on your vision and planning discussed above, you can now develop a map of required bandwidth per region. Confirm the number of wireless users likely to connect in any given area, then determine whether geography or applications will drive bandwidth. It's usually a bit of both. You can use these consumption rates to help estimate your typical traffic:

Email, Web surfing: 50Kbps to 200Kbps – very bursty

VOIP: 100K, full duplex

Video over IP: 2.5Mbps (Mpeg-2) average

Can vary from 500Kbps to 8Mbps

Use broadcast video wherever possible to take advantage of multicast delivery mechanisms that preserve precious wireless bandwidth

Now that you have your regional population and bandwidth estimates, the best way to develop an initial (but fairly accurate) architecture is to utilize the Aruba automated planning tools. Today's generation of planning tools takes most of the guess work out of wireless network design. The tools will determine AP placement based on population density, desired coverage area, performance or a combination of all three. Every environment is different and thus can dramatically affect the wireless architecture and design. Therefore, while interesting, rules of thumb don't come close to giving a reasonable representation of

---

the final architecture and design. Automated planning tools are your best bet in drafting an initial architecture that closely approximates the final result..

To verify your planning results, experience has shown the following to be true:

In a mixed 802.11b/802.11g environment, expect performance between 10Mbps and 15Mbps maximum per channel

Pure 802.11g or 802.11a will yield performance from 20Mbps to 28Mbps per channel

In any case, figure a max of 25 users per AP

Multicast rates (802.11a):

With the lower bound set to a multicast rate of 12Mbps, we were able to obtain four concurrent 2.5Mbps video streams

With the lower bound set to a multicast rate of 24Mbps we achieved up to seven concurrent streams

Remember that the more bandwidth you dedicate to multicast, the less there is available for general purpose traffic. That's why it's better to place more APs in a given region and reduce the number of multicast streams per AP

For the most part, QOS is not an issue. Wireless bandwidth has dramatically improved over the last few years. In addition, APs can tag certain types of traffic, such as VOIP, as high-priority. This can be further enhanced by QOS and Access Control Lists on the wired network to prevent over-consumers of bandwidth or a denial of service attack from blocking the high-priority voice traffic. In general, it's better to prioritize and protect traffic of interest, then serve the remaining traffic as best effort.

Security policy must now be determined. Trying to lock down everything just doesn't scale; the implementations are too complex and create contention between users. Security policy varies widely from user to user, making any kind of generic implementation problematic, at the very least, and most likely impossible. For example, one set of firewall rules may protect a certain environment while restricting others to the point where their systems are unusable. Experience has shown that protecting the environments that you value the most from end to end is the best approach. VPNs are a very simple, highly effective and proven technology to secure communications between endpoints. Adopting 802.1x lends great flexibility to present and future authentication/access controls. If you have an existing Radius infrastructure, it can likely be leveraged for 802.1x support.

Decide on the resources you'd like to protect most. Then use the wireless switch to tag traffic of interest (such as VoIP) to insure it will never be blocked by a malicious denial of service attack. These tags can be backed up by ACLs and VLANs on

---

the wired backbone routers to preserve priority. Then use the integral VPN service termination in the wireless switch to provide scaleable end-to-end encryption of sensitive wireless traffic. That will reduce the number of additional devices to manage while lowering the total system cost of ownership.

Channel planning is becoming more automatic and, for the most part, is handled in the vendor planning tools or by the APs in real-time at start-up. However, for most multi-level buildings, you should be aware that a three-channel, 802.11b/g architecture may not suffice. This is because, in the real world, you are dealing with three-dimensional space, not the two-dimensional planning tool. That means you will experience interference from APs on floors above and below the deployed AP. Going to a four-channel architecture, while not completely eliminating adjacent channel interference, will minimize it much better than a three-channel architecture. In practice, I found no issues with deploying a four-channel architecture if you're careful about placement. You also may need to optimize channel assignment manually. The current generation of Aruba code is better at making these optimizations than previous versions.

If you are deploying a converged network or you anticipate the need to support high-bandwidth or latency-sensitive services, then 802.11a will be in your future. In an enterprise or campus, it is good practice to design coverage areas based on 802.11a. That way you won't have to re-position or add APs to effect 802.11a service.

Location awareness will play a key part in the deployment of presence. Additional APs and air monitors may be required in a given area to support the granularity of location awareness desired.

## Sighting for Optimization and Installation

After completing your initial design with the automated tools, you should conduct a walk-through of planned installation sites. Today's generation of planning tools does not account for variations in construction, building materials, access to proposed AP placement locations, or esthetics. Variation in building materials can affect the propagation of RF, causing it to deviate from your planned coverage. For example, an AP designed to cover three or four rooms may work just fine through sheet rock walls. However, if those walls are actually concrete, the AP signals may not propagate beyond the walls in which the AP is placed. Here's a chart of typical RF attenuation through various materials:

Object	2.4GHz	5 GHz
Interior drywall	3-4dB	3-5dB

---

Cubical	2-5dB	4-9dB
Wooden door	3-4dB	6-7dB
Brick/Concrete Wall	6-18dB	10-30dB
Glass window (not tinted)	2-3dB	6-8dB
Double Pane Coated Glass	13dB	20dB
Bullet-Proof Glass	10dB	20dB
Steel/Fire Exit Door	13-19dB	25-32dB

Depending on building construction, it may not be possible to place an AP where originally planned. But by going to the recommended position for each AP prior to its installation, you can identify these issues in advance, enabling you to re-position the AP in the planning tools and update the design. The alternative—waiting to find obstructions during the installation process—can waste time and money, as re-positioning a single AP at that stage in the process may require the re-positioning of several other APs as well.

If you are deploying Wi-Fi access outdoors, it is often possible to cover many areas from inside. Placing an AP (or directional AP antenna) in a window allows desired coverage while eliminating the expense of a hardened AP. It also makes the AP much more accessible for service when required. Experience has shown that many buildings enclose or adjoin outdoor areas of interest, making this a viable option. Make sure to verify the type of window glass through which your signals will travel. Older buildings may have glass that contains lead, which can affect signal propagation.

When placing APs outdoors, one should pay attention to antenna height. Many think that locating an AP outside on a high point will provide increased or better outdoor coverage. They forget, however, that AP antennas radiate their signals in a pattern that will direct the majority of the signal above the user's head if the AP antenna is located too high.

You have no control over the user's antenna directionality. Even if you can direct the AP antenna downward towards the user, the user's antenna direction likely would still not match yours. Remember that most people (and their laptops) are only four to six feet high and thus, the AP's antenna height should match.

---

Access to network backhaul also can be of concern, especially for outdoor installations. Aruba's AP80 dual radio AP can solve this problem by using one radio for Wi-Fi access and the other for wireless backhaul to your network backbone.

#### Third-party interference

The 802.11 standards upon which Wi-Fi is based encompass license-free RF spectrum. This means that any interference occurring within that spectrum must be tolerated. In other words, you can't control interference from other devices. During your walking tour, determine potential sources of interference. You may have to adjust your AP placement, channel assignments or antenna directionality in order to minimize the interference.

## System Pilot and Installation

It's best to test your architecture and design before beginning your production installation. As RF can be affected by many things, your actual performance may vary from the planned design. If you've done a thorough job gathering requirements and sighting the installation, that variation should be minimal. In any case, it's much less costly to find and correct any major holes in the design before rolling out the entire installation. A pilot will also help to wring out any integration issues with the wired core backbone that may have been overlooked during the design.

In choosing your pilot, select an area from your design to pilot that best pushes the limits of the design. Piloting your system will help you gain experience with the details of installation that are critical to keeping your production installation on schedule. It is also an excellent opportunity to test the support tools for software upgrades and the like. With the potential to deploy thousands of APs, your support tools are a critical factor in maintaining system availability and can help maximize the use of limited personnel. If you can't successfully configure or upgrade 100 pilot APs, there's no way you'll be able to support 2000. It's well worth the time to test your configuration and software upgrade tools across a large number of APs in the pilot.

Once you've achieved a successful pilot, starting a systematic production rollout is prudent. You may still encounter problems specific to a site and you will want to avoid multiplexing personnel between sites during production installation.

## System Operation, Maintenance and Growth

Once in production you'll need tools to assist with monitoring your wireless network's performance. In addition to the Aruba tools, it is good practice to have third-party tools on-hand to verify results as well as troubleshoot various problems or situations. There are a variety of excellent tools available for a fee or for free. The AirMagnet tools are perfect for debugging

---

RF problems in the field as well as tracking down offending rogue APs or wireless clients. Kismet, an open source tool, is a great platform upon which to build customizable tools. Experience has shown that checking the performance and availability of your wireless system from the client's perspective is the ultimate indicator of your system's health. While not available "off the shelf" today, it is fairly easy to use open source tools to develop wireless probes that act as wireless clients. When placed in strategic locations, these probes can be programmed to associate with every AP in your network over the course of a day to check access and to report on performance. Taking a proactive approach allows you to find problems before your users do and will help you to maintain high availability in your wireless network.

---

## Executive Bio of S. Bradley Noblet

Brad Noblet is a veteran Information Technology executive of thirty years. His breadth of experience extends from managing the development, delivery and support of IT products to forming and leading major IT companies. Over the last six years he has successfully leveraged his industry management experience toward delivering high quality, visionary IT environments for Higher Education. During that time, Brad served as Dartmouth College's Director of Technical Services then becoming its CIO. At Dartmouth he was responsible for creating the College's and the industry's first enterprise class converged (voice, video and data) network in addition to advancing and managing its central IT operations. His vision for IT, reflected in the infrastructure, applications and services he deployed while at Dartmouth brought much recognition to the College from industry, Higher Education and the national press touting Dartmouth as a leader in IT.

A 1982 graduate of Indiana University at Bloomington in Computer Science, Brad was that school's Manager of Data Communications, with responsibility for the institution's statewide data network. He then left for private industry, working in product development and management for a number of hardware manufacturers including Codex Corp., Ungermann-Bass, Tandem Computers and the Wellfleet Communications division of Bay Networks.

At Ungermann-Bass, Brad served as Director of Engineering then General Manager of several business units. He is credited with the creation and development of Ungermann Bass' flagship product, Access/One, the world's first smart hub. He joined the Wellfleet Division of Bay Networks in 1995 as General Manager of that business unit delivering over \$600 million in annual revenue. He is credited with creating forty new products during his tenure at Wellfleet that resulted in growing its revenue by \$200M in less than two years.

Since leaving Bay Networks in 1998 and before joining Dartmouth in 2001, Brad was involved in a number of start-up ventures focused on the converged voice, data and wireless sectors. He is regularly quoted in industry journals and the national press, being touted as an expert in networking and provides consultation for several Fortune 500 companies and Higher Education institutions.

---

## About Aruba Networks

Aruba securely delivers the enterprise network to users, wherever they work or roam, with user-centric networks that significantly expand the reach of traditional port-centric networks. User-centric networks integrate adaptive WLANs, identity-based security, and application continuity services into a cohesive, high-performance system that can be easily deployed as an overlay on top of existing network infrastructure. Adaptive WLANs deliver high-performance, follow-me connectivity so users are always within reach of mission-critical information. Identity-based security associates access policies with users, not ports, to enable follow-me security that is enforced regardless of access method or location. Application continuity services enable follow-me applications that can be seamlessly accessed across WLAN and cellular networks. The cost, convenience, and security benefits of user-centric networks are fundamentally changing how and where we work. Listed on the NASDAQ and Russell 2000® Index, Aruba is based in Sunnyvale, California, and has operations throughout the Americas, Europe, Middle East, and Asia Pacific regions. To learn more, visit Aruba at <http://www.arubanetworks.com>.

© 2007 Aruba Networks, Inc. All rights reserved. Aruba Networks, BlueScanner and RFprotect are trademarks of Aruba Networks, Inc. All other trademarks or registered trademarks are the property of their respective holders. All rights reserved. Specifications are subject to change without notice.

WP\_EDDAR\_US\_071217

